TalkTalk response to ICO Age Appropriate Design
May 2019

1. Introduction to TalkTalk

1.1. TalkTalk is the UK's challenger telecoms company, providing landline, broadband and TV to over 4 million customers. We operate Britain's biggest unbundled broadband network, covering 96% of the population, supplying services to consumers through the TalkTalk brand and to businesses through TalkTalk Business and also by wholesaling to resellers.

1.2. We are committed to building a safer online world for customers and recognise that safeguards are needed for children when accessing the internet. TalkTalk was the first UK ISP to introduce free parental filters for all customers, a policy which has subsequently been adopted by all major UK ISPs. We are also founding members of Internet Matters, a not for profit organisation dedicated to helping families keep their children safe online, and work with it to ensure our customers have the tools and confidence to safely navigate the online world.

2. General view on the Code

2.1. TalkTalk is pleased to comment on the ICO's draft Code of Practice for online services on Age Appropriate Design. We are passionate about the benefits of the internet, but recognise that customers need support to safely navigate the online world. Technology companies have a responsibility to foster a safer online world by helping customers to understand online risks and ensuring products and services are designed with safety as a priority.

2.2. Based on these principles, TalkTalk believes the ICO's new Code of Practice offers an opportunity to ensure that safety is a core principle of all innovation. This would both deliver positive outcomes for consumers, particularly the most vulnerable, and also could unlock a new era of technological development. Therefore, we supported the introduction of the Code at the legislative stage and have since responded to the summer 2018 Call for Evidence, supporting many of the principles included in the Code and commending the ICO's ambitious approach.

2.3. However, we have some concerns about this initial draft of the Code, mainly related to uncertainty regarding the scope, which we hope to see clarified. The Code as currently drafted can be clearly understood in the context of online platforms such as social media sites, gaming platforms and connected devices where individual users have a direct relationship with the service provider and are "likely to be accessed by a child". We have no comments on the specific application of the Code to these services, beyond general support for regulatory best practice and a proportionate approach to regulation.

2.4. However, it is not clear how an ISP could look to be compliant with the Code as currently drafted. As such, we understand that connectivity services provided by Internet Service Providers (ISPs) will not be included within the Code's scope. We explain our rationale at section 3.1.1-7; however, we would welcome confirmation from the ICO that ISPs will not be in scope of the final Code.

2.5. The Code also comes at a crucial moment for the UK internet industry as it follows the Government's Online Harms White Paper. We support the proposals of the White Paper and welcome the Government's emphasis on the need for effective policies and processes, underpinned by appropriate regulatory functions, and which is informed by a live understanding of harms. The Age Appropriate Design Code is highly relevant to the system envisaged by the White Paper and therefore it would be helpful if the ICO and DCMS set out how they envisage the two regulatory processes working together.

2.6. We also hope for continued engagement between industry and the ICO after this consultation window, and it will be important that the implementation window is sufficient to allow industry to introduce any new processes required by the Code correctly and in an orderly fashion.

2.7. We have not responded to each question in the consultation survey; however, we have indicated which question each section refers to.

3. Comments on scope (Question 2)

3.1. Connectivity services

3.1.1. We believe the Code should be clearer on which services are in scope to build greater understanding and confidence in the Code.

3.1.2. The legislation defines the Code as applying to "relevant information society services which are likely to be accessed by children". However, this definition is not reflected across the rest of the paper as the content largely relates to activities by platforms such as social media sites, apps and connected toys. ISPs are deemed to be information society services (ISS) under the terms of the E-Commerce Directive and therefore would be expected to comply with the Code; however, as written, it is not clear how an ISP could demonstrate compliance with the Code as they do not offer the features or services referred to by the ICO.

3.1.3. The code refers to "users", not customers – whereas an ISP only has a direct relationship with a named customer, who is over 18, and only able to sign a contract if they are over 18 (which is verified through credit rating checks etc.) An ISP provides a household connection service which may have many users over time; however, the ISP has no visibility of these individual users/ devices. Therefore, any information collected or processed is at the IP address level, and is not matched with any other data to establish individuals within a household. We also actively take steps to minimise data collection- for example, through the provision of a Domain Name Server (DNS) we capture extensive details about websites visited by customers. However, this is retained for only a very short period of time and is aggregated to inform cybersecurity activity at a network level, but it is not used at a customer level or for commercial purposes. Therefore, as ISPs do not collect or process data on an individual basis, our understanding is that connectivity services are outside the scope of the Code.

3.1.4. Furthermore, the Code says that it is for companies which are "*providing online products or services… [that] are likely to be accessed by children in the UK*". This would include ISPs as it provides a service which is likely to be accessed by children – i.e. basic connectivity which is essential for any further online activity. It is unclear how the Code

could apply to basic connectivity services – for example, geolocation options are not applicable because our services are provided only to fixed lines.

3.1.5. We believe this interpretation is in line with the original intention of the debate. For example, the original Parliamentary debates which led to section 123 of the Data Protection Act 2018 which underpins the Statutory Code focused on specific instances of data collection, such as that which included a "*child's school or home address, their birth date, their likes, dislikes, friends or photographs, in order to facilitate a specific activity being undertaken by that child*"[1]. ISPs collect no such information about any of their users, whether children or adults. The focus of the Code is – rightly – on those services which collect and process significant volumes of data and where the risk to the child's rights are higher. This is not the case with connectivity services.

3.1.6. Based on this reading of the Code, we believe that TalkTalk's connectivity services are outside the scope of this consultation. This should be clarified and confirmed in the final version. There is a significant risk to companies from non-compliance and therefore it is essential that ISPs can be confident in their assessment of the Code. We would welcome further engagement with the ICO on this point.

3.1.7. However, if the Code is intended to cover ISP's connectivity services, it should be revised to provide an assessment of how it applies to these types of services, with specific examples of compliance included. This will require significant amendment to the Code and continued engagement with industry on this issue, including a further consultation period.

3.2. *Other services*

3.2.1. Our reading of the Code is that TalkTalk's TV service would be in scope as it provides content streaming services, as would the Video of Demand (VOD) apps that we host on our platform. We would welcome clearer guidance from the ICO about what appropriate steps are needed to be compliant with the Code.

3.2.2. We would also reiterate the need for the principle of proportionality to be considered when judging compliance in this case. Any measures should be designed to address clearly-evidence harm categories and consider what is a proportionate response, rather than set prescriptive requirements for platforms to follow in all cases. For example, the Code highlights auto-play as a user engagement strategy used by content providers, and says these should not be used with children at present. A blanket approach against all auto-play, regardless of length of content, seems to us to be overly prescriptive – a more proportionate approach would be to set a maximum time period when auto-play could be used, for example.

3.2.3. The ICO should also recognise that VOD services are already regulated by Ofcom under the Audio-visual Media Services Directive. The ICO should recognise that this regime entails a number of standards to protect children (for example age-gating certain material and ensuring that prohibited material does not appear, while the updated 2018 Directive prohibits providers from processing minors' personal data for

[1] Baroness Kidron, House of Lords Debate, 11 December 2017, c1426

commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising). This is quite different from many online content streaming services and the distinction between the two should be recognised when applying the Code. The final Code should set out how it will not duplicate or counteract current regulatory standards, perhaps through a Memorandum of Understanding.

3.3. ***Parental controls***

3.3.1. As we have expressed above, it is difficult to understand how the ICO intends the Code to apply to ISPs. One particular example is around parental controls. While we do not object to the ICO's proposals on parental controls, they are written in reference to app-based parental controls, rather than ISP network level controls – which block inappropriate content rather than actively monitoring usage for review by a parent. We would welcome clarity on whether or not network-level filters are in scope in the final version of the Code and, if they are, with clear expectations of what is required by ISPs.

3.3.2. For example, it is not clear how ISPs could implement the second recommendation on parental filters – a requirement to alert children when tracking services are in use – as parental filters on fixed connections do not operate "in the background" like app-based controls. Therefore it would be helpful to clarify that network-level parental controls would not be required to implement this recommendation.

4. Proportionality (Question 1/ Question 5)

4.1. More generally, the ICO should take a proportionate approach to implementing this Code – determined by the type and volume of data collected, and the potential risk to children. This proportionate approach, which requires more from platforms where the potential for harm is greatest, aligns with the Government's Online Harms White Paper and is a sensible approach to prevent significant harm from occurring.

4.2. To be clear, we are not arguing for small businesses to be excluded from the Code entirely; we believe the Code is a good opportunity to embed safety by design as a principle in from the ground up, and has the potential to unleash a new wave of technological innovation to make the UK a world-leader in a trend that it likely to expand across the world. However, proportionality will ensure that regulation applies where it is most needed and does not constrain other features or practices which are not harmful.

4.3. The ICO should make a clear statement in favour of proportionality and give guidance on how it will shape its regulatory approach. The ICO should make clear that the nature of the data collection, the purpose behind it and the risk children could be exposed to should be taken into account in coming to a judgment in relation to the Code. It should also take a proactive approach to engagement with business to help them understand activities which are in and out of scope.

5. Risk of unintended consequences (Question 5)

5.1. We also raise the risk of unintended consequences from the Code if it leads to more data being collected from children. Data minimisation is one of the guiding principles of GDPR;

however, the draft Code's requirement on companies to provide evidence as to whether their service is "*likely to be accessed by a child*" risks seeing increased data collection and analysis to understand more about users. For example, if TalkTalk wanted to demonstrate that our homepage is not likely to be accessed by a child, we would likely need to collect information about current users to infer the age and other profile characteristics of users.

5.2. Not only would this require ISPs to fundamentally redesign their products – to create individual accounts for each user – this would go against the spirit of the Code in entailing more detailed collection and profiling than is currently the case.

5.3. ISPs have steered away from collecting individual user data and instead operate as a household service, holding a relationship with a named account-holder. Therefore, our safe design principles have been implemented at a household level, such as our filters which apply across the network rather than on specific devices. All accounts have the ability to switch on free parental control filters which allow the account-holder to filter sites and content across the network.

5.4. Therefore, we would welcome clarity on how the principle of data minimisation applies to the Code.

6. Feasibility requirements and implementation period (Question 7)

6.1. We are concerned that the ICO is overly ambitious in its proposed timing. The standard three month implementation period will very likely be insufficient to allow businesses to implement changes in order to be compliant. In many cases compliance will involve re-designing products, and the technical changes and testing processes are likely to take 9-12 months. The ICO should publicly recognise that compliance will be complex and dependent on significant resources. Industry should have at least a year to implement changes once the Code is finalised.

6.2. The Code has been open for public consultation for six weeks; while we appreciate this chance to comment on the current draft, our view is that this period was not sufficient to allow businesses to fully consider the impact of the Code and consult with the ICO and third parties as required. Therefore, the ICO should commit to a further period of industry engagement – not necessarily in a formal consultation process but perhaps a series of formal meetings with industry representatives– ahead of publication of the final Code.

7. Recommended way forward

7.1. To summarise, the final draft of the Code should:

- Clarify that ISPs' household connectivity services are excluded from the scope of the Code.
- Restate and strengthen the principle of proportionality, but indicating how the Code will assess the likelihood of harm and how this assessment will influence regulatory decision.
- Acknowledge potential for overlap both with future regulatory processes suggested in the Online Harms White Paper and set out how the proposals will align with current regulation of Video on Demand services and online advertising.